ABSTRACT

A 'virtual' encryption scheme combines selected ones of plurality of different encryption operators stored in an encryption operator database into a compound sequence of encryption operators. Data to be transported from a data source site, such as a user workstation, to a data recipient site, such as another workstation, is sequentially encrypted by performing a compound sequential data flow through this sequence prior to transmission. Because of the use of successively different encryption operators, the final output of the sequence will be a compound-encrypted data stream that has no readily discernible encryption footprint. Therefore, even if a skilled data communications usurper possesses a decryption key for each encryption operators, there is a very low likelihood that he would be able to recognize the characteristics of any individual encryption operator. Moreover, without knowledge of the sequence of encryption operators a potential usurper will be forced to operate under a severe resource penalty that makes decryption of such a compound sequence a practical impossibility. At the recipient end of the data communications path, the recovery process involves the use of a complementary virtual decryption scheme that is the exact reverse of that used at the data source site.